epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of

Marc Rotenberg, Executive Director
And
Ruchika Agrawal, IPIOP Science Policy Fellow
Electronic Privacy Information Center (EPIC)

Workshop on
Technologies for Protecting Personal Information:
The Consumer Experience
and
Technologies for Protecting Personal Information:
The Business Experience

Before the

Federal Trade Commission

May 14, 2003 and June 4, 2003
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC

A meaningful discussion of the intersection of privacy and technology must be preceded by answers to the following questions:

- What is privacy?
- How should technology be designed to safeguard privacy? Or, what are privacy enhancing techniques?
- What are examples of technologies or techniques that safeguard privacy?
- What are technologies that do not safeguard privacy?
- What are common characteristics of techniques that safeguard privacy?
- What is the future of designing technologies that safeguard privacy?

We will begin by answering the first three questions in turn, and then consider the remaining questions as appropriate.

Understanding Privacy

Privacy is a civil liberty. Your privacy is your freedom to move in and out of the public sphere. One aspect of privacy addresses control of your own personal information, control over what others (other people, private organizations, and the government) know about you, and control over how others may use or exploit your personal information. [26] In Olmstead v. U.S. (1928), Justice Louis Brandeis described privacy as "The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people." Privacy may also be understood as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves." [25]

In the modern era, privacy has often been described as “Fair Information Practices.” Fair Information Practices minimize the collection of personally identifiable information, and enable control over personal information by outlining rights of users and responsibilities of services in the collection of personally identifiable information. Organizations that acquire information about individuals have certain obligations, such as the responsibilities to ensure that personal information is accurate and complete, and not disclosed or used for an improper purpose. Individuals have certain rights, including the right to access their personal information, to make corrections if necessary, to understand how it will be used and to object to its misuse. These Fair Information Practices are found in many laws around the world. [23] For example, see the Canadian Standards Association’s Model Code for the Protection of Personal Information. [7]

Central to the definition of privacy is the concept of anonymity. [26] Policies and practices that respect privacy aim at minimizing the collection of personally identifiable information. [26] Then intuitively, the starting point of privacy is anonymity, where no personally identifiable information is collected.

Privacy is also critical to free speech. [18, 26] As a simplified explanation, if speakers are compelled to disclose their identity, speakers are reluctant to fully express their speech for fear of persecution or discrimination. We established that the pinnacle of privacy is anonymity; hence, as a corollary, anonymity is critical for individuals to achieve their fullest ability to exercise free speech. The importance of anonymity to free speech has been recognized by the United States Supreme Court. *See* McIntyre v. Ohio, 514 U.S. 334, 343 (1995). Therefore, techniques that achieve anonymity also achieve privacy and enhance free speech.

Architecting Privacy: Privacy Enhancing Techniques

Technology can be designed to safeguard privacy. Here, we will generally refer to such design principles as Privacy Enhancing Techniques (PETs).[1] PETs eliminate or minimize the collection of personally identifiable information. [26]

We use PETs in everyday life. Cash, for instance, enables us to purchase items and services without transferring any personally identifiable information. It gives us the freedom to engage in commerce without disclosing our actual identity to others. Stamps allow us to send mail. With a few coins, we can make calls from a payphone. Similarly, metro cards and movie tickets allow individuals to gain access to services without creating a trail of personally identifiable information.

The key intuition behind understanding PETs comes from asking the following questions: when is the collection of personally identifiable information necessary, how much data collection is absolutely necessary to complete a transaction or a communication, and when is it necessary to identify an individual? To fully appreciate any answer to these questions, we must first make a distinction between identifying and authorizing -- e.g. movie tickets authorize us to watch a particular showing of a movie without identifying us. [22]

It is our view that the development and application of PETs will be a critical requirement for the safeguarding of privacy in the twenty-first century. Visa International is already headed in this direction with their recently announced plans to establish a new policy that would prohibit the display of all but the last four digits of a credit-card number on consumer receipts to better protect consumer privacy. [2]

Examples of PETs

The following PETs can provably eliminate or minimize the collection of personally identifiable data while enabling transactions or communications, given that they overcome certain challenges.

- **Anonymous Publication and Storage Services**. Anonymous publication and storage services enable users to speak freely without being identified. A net of servers storing pieces of documents provide the infrastructure. A reputation-based system enables trust among servers to store and retrieve pieces of documents dynamically. [12]

[1] We have previously referred to 'PETs' as 'Privacy Enhancing Technologies'. However, 'Privacy Enhancing Techniques' is a much broader term that conceptually appeals to examples that go beyond technology.

The effectiveness of anonymous publication and storage services depends on the implementation and the practices of the service provider. For example, the implementation should not at any point attempt to link the publication to the speaker. The effectiveness of anonymous publication and storage services also depends on the practices of the user, who should not reveal personally identifiable information in the content of the publication.

- **Anonymous Remailers**. An anonymous remailer is a computer program that allows users to anonymously send emails and post to newsgroups. [19] Anonymous remailers are similar to email server software, except that remailers do not log incoming and outgoing traffic information and remailers strip email headers of personally identifiable information. [19]

  The effectiveness of anonymous remailers depends on the implementation and the practices of the vendor. For example, the vendor should not secretly log all incoming and outgoing traffic in its implementation of an anonymous remailer. The effectiveness of anonymous remailers also depends on the practices of the user, who should not reveal personally identifiable information in the message subject or body.

- **Digital Cash**. Hard cash serves as a model for digital cash, enabling users to pay for goods and services without being identified. A digital cash system may consist of three entities: (1) digital cash issuers and validators (e.g. digital cash banks); (2) customers who would establish accounts with such banks; and (3) goods or service providers that would accept digital cash payments. [8] Blind signatures and public-key cryptography are essential infrastructure elements ensuring anonymity and security. [4, 8] Digital cash serves as a good example of an effective PET, since digital cash eliminates the collection of personally identifiable information.

  The effectiveness of digital cash depends on the implementation and the practices of the digital cash issuer. For example, the issuer should not record and link your identity with the serial number of the digital cash when he issues it to you, which could enable data collection at the time the digital cash is used.

- **Digital Credentials**. Digital credentials enable users to selectively disclose information from their digital credentials, thereby proving certain assertions about themselves without revealing unnecessary personally identifiable information to a service that is collecting personally identifiable information. [3] For example, a user may disclose that he is a student and is therefore eligible for some benefits without revealing more information. Digital credentials may be implemented as a collection of digital certificates underpinned by a public and private key infrastructure. [3]

- **Digital Tickets**. Digital tickets are digital certificates that guarantee certain rights to the ticket-holder. [14] Digital tickets enable commerce and communication while limiting the collection of personally identifiable information. Our physical world provides ample evidence of the effectiveness of this approach. The use of movie tickets, for example, authorizes a ticket-holder to watch a particular showing of a movie without the collection or recording of the ticket-holder's personally identifiable information. [22] Digital tickets serve as a good example of an effective PET, as they eliminate the collection of personally identifiable information.

The effectiveness of digital tickets depends on the implementation and the practices of the ticket issuer. For example, the issuer should not record and link your identity with the serial number of the digital ticket when he sells it to you, which could enable data collection at the time the ticket is used.

- **Encryption of Disk, Email, File, Instant Messaging, Telnet, and Web Information**. While encryption is employed to ensure anonymity and privacy at various levels, one aspect of encryption minimizes the collection of personally identifiable information by making the information unintelligible to data collectors before data is collected. Encryption of disk, email, file, instant messaging, telnet, and web information also enhances security by inhibiting unauthorized parties from gaining access to the data content. [10, 11, 15, 17, 22, 24, 27]

- **Pre-paid Smart Cards**. A prepaid smart card enables the cardholder to purchase goods and services without being identified. [9] Pre-paid calling cards illustrate this technique. A customer purchases a pre-paid calling card, the calling card authorizes the customer to make calls for a certain amount of time, and the customer uses a PIN to become authorized. The signature-transporting card, one of four kinds of smart card technologies, is the most effective approach in protecting privacy by avoiding the need for identification. [9] A signature-transporting card stores publicly verifiable digital signatures created by the smart card provider, and uses a different signature for each payment. [9]

  The effectiveness of pre-paid smart cards depends on the implementation and the practices of the vendor. For example, the vendor should not record and link your identity with the serial number of the smart card when he sells it to you, which could enable data collection each time the card is used.

- **Techniques that Purge/Delete Data.** Techniques that facilitate the purging or deleting of data minimize the collection of personally identifiable information. For example, Apple recently released X11 (the X Window System that runs UNIX applications), and a new browser (Safari). The browser enables users to easily clear cache, history files, and downloads (note that the "clear" button is placed right next to the file list), and pop-up ads are automatically blocked. As another example, the first publication of *IEEE Security & Privacy* included an article on disk sanitization techniques – including sanitizing through erasing and overwriting – based on the premise that many discarded hard drives contain information that is both personal and recoverable. [17] As a final example, libraries routinely destroy patron borrower records to preserve privacy.

  Several privacy laws that aim at minimizing data collection include explicit data destruction provisions. For example, the Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002)) generally prevents disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material." The Act has several important provisions, including a requirement that video stores destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information. [28] Similarly, the Cable TV Privacy Act of 1984 requires that a cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information. [6] Finally, the European Union Data Protection Directive requires that personal data be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they are further processed. [23]

In this respect, techniques that facilitate data purging or deletion to minimize the collection of personally identifiable information would be considered PETs.

- **Web-Surfing "Anonymizers"**. Web-surfing anonymizing tools enable users to surf the web without being tracked, monitored, profiled or exposed to unwarranted cookies, damaging viruses, and unsolicited popup advertisements. [16] Users can visit websites through anonymizing software (as opposed to standard browsers), [16] which for example, encrypt URLs to circumvent network logging. [1] Because network logging is necessary to some extent – for example, to deliver HTTP requests – we consider web-surfing anonymizers as PETs that minimize the collection of personally identifiable information.

  The effectiveness of web-surfing anonymizers depends on the implementation and the practices of the vendor. For example, the vendor should not secretly log unencrypted URLs in its implementation of a web-surfing anonymizer.

P3P: A Non-PET Example

While PETs are a simple concept (as cash, movie tickets, and metro cards demonstrate), they are sometimes misunderstood.

A number of technologies are falsely presented as PETs, but do not actually satisfy the definition of PETs. In particular, The Platform for Privacy Preferences (P3P), widely described as a privacy technology is not a PET.

P3P requires websites to specify their privacy policies in a machine-readable format, for example, XML. [29] Though not required by the P3P protocol, client tools, such as Internet Explorer 6.0 and the AT&T Privacy Bird, may enable users to specify their privacy preferences so that P3P clients may read a website's privacy policy, determine whether the policy satisfies a user's privacy preferences, and warn the user if not. [29] Privacy Enhancing Techniques, on the other hand, minimize the collection of personal data and thus result in far fewer collections of personally identifiable information. [5]

P3P fails as a privacy enhancing technique because P3P does not aim at protecting personal identity, does not aim at minimizing the collection of personally identifiable information, and is on a completely different trajectory than the one prescribed by the definition of PETs. [13] P3P provides no genuine privacy protection: [13, 21] instead of being used to minimize the collection of personally identifiable information, P3P can easily be used to obtain data from consumers by facilitating the collection of personal information through the guise of notice and choice. [20]

We note the problem with P3P because much of the recent discussion on privacy technologies has focused on this protocol. We believe better standards should be developed for privacy protection. This process requires a careful articulation of the characteristics of techniques that truly safeguard privacy.

CONCLUSION

Our discussion of PETs demonstrates that technology can be designed to assist in safeguarding privacy. There are several characteristics common to the various PETs described. For example, all PETs:

- limit the collection of personally identifiable information;
- enable commerce and communication;
- do not facilitate the collection of personal information;
- do not force Internet users to trade privacy to participate in commerce or communications; and
- do not treat privacy as a business commodity.

These are all desirable characteristics that genuinely advance privacy and promote transactional activity in the online environment. For these reasons, we believe that PETs are both an effective solution to counter prevalent privacy threats and to promote the use of new services.

The critical question for PETs is the definition. Some have said that to give consumers "choice" about a privacy policy is a form of PET. But these methods for contracting do little more than automate marketplace negotiations, and oftentimes force consumers to trade personal information to obtain a product or service. A better approach should build privacy into the service, much like seatbelts and airbags are built into cars.

Genuine PETs eliminate or minimize the collection of personally identifiable information, thereby providing a non-negotiable level of privacy.

The challenge ahead is to simplify PETs so that they are in reach of the average user. The implementations should be robust, reliable, and widespread. In other words, the use of PETs should be as simple as the use of cash, movie tickets, and metro cards. We recommend further research and funding in simplifying PETs in this direction.

REFERENCES

[1] Anonymizer.com; http://www.anonymizer.com/ (visited on October 22, 2002).

[2] Chris Baker; "Visa moves to improve customers' privacy"; *The Washington Times*, March 6, 2003; http://washingtontimes.com/business/20030306-3647521.htm.

[3] Stefan Brands; "A Technical Overview of Digital Credentials"; February 20, 2002; http://citeseer.nj.nec.com/brands02technical.html.

[4] Stefan A.Brands; "Untraceable Off-line Cash in Wallets with Observers"; *Advances in Cryptography-CRYPTO '93*; Springer-Verlag; 1994; p.302-318.

[5] Herbert Burkert; "Privacy-Enhancing Technologies: Typology, Critique, Vision"; Technology and Privacy: The New Landscape edited by Philip Agre and Marc Rotenberg; The MIT Press (Cambridge, 1997).

[6] Cable TV Privacy Act of 1984; 47 U.S.C. § 551.

[7] Canadian Standards Association; Model Code for the Protection of Personal Information (CAN/CSA -Q830-96); 1995; http://www.csa.ca/standards/privacy/code/Default.asp?language=English

[8] David Chaum; "Achieving Electronic Privacy"; *Scientific American*, August 1992; p. 96-101; http://ntrg.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html.

[9] David Chaum; "Prepaid Smart Card Techniques: A Brief Introduction and Comparison"; Digicash; 1994; http://ntrg.cs.tcd.ie/mepeirce/Project/Chaum/cardcom.html.

[10] Roger Clarke; "Roger Clarke's PITs and PETs Resources Site"; http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html#Orig (visited on October 21, 2002).

[11] Whitfield Diffie and Martin E. Hellman; "New Directions in Cryptography"; *IEEE Transactioins on Information Theory*; IT-22(6); November 1976.

[12] Roger Dingledine, Michael J. Freedman, David Molnar; "The Free Haven Project: Distributed Anonymous Storage Service"; December 17, 2000; http://citeseer.nj.nec.com/543510.html.

[13] Electronic Privacy Information Center in association with JunkBusters; "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy"; June 2000; http://www.epic.org/reports/prettypoorprivacy.html.

[14] Ko Fujimura and Yoshiaki Nakajima; "General-purpose Digital Ticket Framework"; Proceedings of the 3rd USENIX Workshop on Electronic Commerce; August 31-September 3, 1998; http://citeseer.nj.nec.com/430527.html; p. 2.

[15] Simson Garfinkel; PGP: Pretty Good Privacy; O'Reilly & Associates, Inc. (Sebastopol, 1995).

[16] Simson Garfinkel with Gene Spafford; Web Security, Privacy & Commerce; O'Reilly & Associates, Inc. (Beijing, 2002); Second Edition; p. 262-283.

[17] Simson L. Garfinkel and Abhi Shelat; "Remembrance of Data Passed: A Study of Disk Sanitization Practices"; *IEEE Security & Privacy*; January/February 2003.

[18] McIntyre v. Ohio, 514 U.S. 334, 343 (1995).

[19] Ceki Gulcü and Gene Tsudik; "Mixing E-mail with BABEL"; IBM Research Division, Zurich Research Laboratory; Symposium on Network and Distributed Systems Security; 1996; http://www.isoc.org/conferences/ndss96/sndss96.htm.

[20] Marc Rotenberg, Director of Electronic Privacy Information Center; Hearing on S. 809, The Online Privacy Protection Act of 1999, Before the Subcommittee on Communications Committee on Commerce, Science and Transportation, U.S. Senate; July 27, 1999; www.epic.org/privacy/internet/EPIC_testimony_799.pdf.

[21] Marc Rotenberg, Director of Electronic Privacy Information Center; "Privacy in the Commercial World"; Prepared Witness Testimony, The House Committee on Energy and Commerce, W.J. "Billy" Tauzin, Chairman; March 1, 2001; http://energycommerce.house.gov/107/hearings/03012001Hearing43/Rotenberg68.htm.

[22] Marc Rotenberg; "A Way Forward for Data Protection: Privacy Enhancing Technology"; *the* PARLIAMENT *Magazine*; September 30, 2002.

[23] Marc Rotenberg, Privacy Law Sourcebook: United States Law, International Law, and Recent Developments (EPIC 2002).

[24] Bruce Schneier; Applied Cryptography; John Wiley & Sons, Inc. (New York, 1996); p. 126-127, p. 220-222, and generally.

[25] Robert E. Smith; Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet; Privacy Journal (Providence, 2000); p. 6.

[26] Daniel J. Solove and Marc Rotenberg; Information Privacy Law; Aspen Publishers (New York, 2003; p. 27-33, 427-37, and generally.

[27] Peter Wayner; Translucent Databases; Flyzone Press (Baltimore, 2002); p.13, p. 129-131, and generally.

[28] The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

[29] World Wide Web Consortium (W3C); *Platform for Privacy Preferences (P3P) Project*; last revised October 23, 2002; http://www.w3.org/P3P/.